AO 106 (Rev. 04/10) Application for a Search Warrant (Modified: WAWD 10-26-18)

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* SUBJECT DEVICE 1 and SUBJECT DEVICE 2	)	Case No. MJ20-533

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

The SUBJECT DEVICE 1 and SUBJECT DEVICE 2 as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. § 545	Smuggling of Goods into the United States
Title 19, U.S.C. § 1595(c)(2)(A)	Merchandise Introduced Contrary to Law
Title 18, U.S.C. § 541 and 542	Entry of Goods Falsely Classified and by Means of False Statements

The application is based on these facts:

✓ See attached Affidavit continued on the attached sheet

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Special Agent Eric Chin, HSI

Printed name and title

○ The foregoing affidavit was sworn to before me and signed in my presence, or

◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 08/19/2020

Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge

Printed name and title

USAO #2020R00630

ATTACHMENT A

Devices To Be Searched

a. A gray OnePlus cellphone, IMEI number 864737041270887, belonging to Colby SMITH, ("**SUBJECT DEVICE 1**"), and

b. A gray Toshiba Laptop Model S75-A7221, belonging to Colby SMITH, ("**SUBJECT DEVICE 2**").

The **SUBJET DEVICES** are currently located in the secure evidence vault of Immigration and Customs Enforcement located in Seattle, WA. Further, the devices have either been shut off or placed into "Airplane Mode" to preserve device contents and the state of the device as seized.

ATTACHMENT B

List of Items to be Searched for and Seized in the SUBJET DEVICES

The following items, which constitute fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, §545 (Smuggling of Goods into the United States), Title 19, United States Code, §1595a(c)(2)(A) (Merchandise Introduced Contrary to Law), Title 18 United States Code §541 (Entry of Goods Falsely Classified), and Title 18 United States Code §542 (Entry of Goods by Means of False Statements), including:

1. All records on the **SUBJECT DEVICES** described in Attachment A that relate to violations of Title 18, United States Code, §545 (Smuggling of Goods into the United States), Title 19, United States Code, §1595a(c)(2)(A) (Merchandise Introduced Contrary to Law), Title 18 United States Code §541 (Entry of Goods Falsely Classified), and Title 18 United States Code §542 (Entry of Goods by Means of False Statements) and involve Colby SMITH, including:

   a. Lists of customers and related identifying information;

   b. Any and all financial accounting records to include check registers, general journals, and supporting journals, logs, spreadsheets, general ledgers, schedules, checks, remittance advices, receipts, invoices mailings, envelopes, tax returns, financial statements and other related documentation involving the buying and selling of Kamagra Sildenafil Oral Jelly, or pharmaceuticals and supplements suspected to contain sildenafil from February 5, 2019 to present;

   c. Any and all bank account records and other information showing the receipt and disbursement of funds to include cancelled checks, deposit and withdrawal slips, cashier's checks, advice of debit/credit, and orders for telegraphic or electronic payment or transfer; safe deposit box numbers and entry records; certificates of deposit, bonds, notes and/or acceptances; wire transfers, bank statements, account applications and all other bank

documents including correspondence, notes, and memoranda, related to transactions, persons or business entities, or accounts from February 2019 to present;

d. Evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

e. Evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

f. Evidence of the lack of such malicious software;

g. Evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

h. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

i. Evidence of the times the digital device or other electronic storage media was used;

j. Passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

k. Documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

l. **SUBJECT DEVICE 1** may be searched only for the following items:

    i. Assigned number and identifying telephone serial number (ESN, MIN, IMSI, or IMEI);

ii. Stored list of recent received, sent or missed calls

iii. Stored contact information;

iv. Stored files (including photographs and videos) displaying or accounting for currency, banking transactions, financial records, shipping information, mail, evidence of the aforementioned offense, and/or that may show the user of **SUBJECT DEVICE 1** and/or coconspirators, including any embedded GPS data associated therewith;

v. Stored text message and stored emails that are evidence of the aforementioned crimes, including similar messaging services saved by third party applications stored on the telephone (such as WhatsApp, Signal, Wickr, and Telegram);

vi. Evidence of user attribution showing who used or owned **SUBJECT DEVICE 1** at the time the items described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, and documents;

vii. Records and information evidencing bank transactions;

viii. Records of Internet Protocol (IP) addresses used;

ix. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user typed web addresses

m. Any mail, packaging, shipping or receiving documents, records, documents or communication, in whatever form, that refer to shipments by Colby SMITH that are part of the smuggling scheme relating to the above crimes;

When executing the warrant, the United States may use the passwords provided by the user of the **SUBJECT DEVICES** at the time it was seized by law enforcement agents.

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, ERIC CHIN, being duly sworn under oath, depose and say:

INTRODUCTION

1. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigation ("HSI"), and have been so employed since March, 2019. I am currently assigned to the HSI Seattle Office. In this capacity, I investigate federal violations including commercial fraud, intellectual property crimes, money laundering, wire fraud, bank fraud, document fraud, and organized criminal activity.

2. Prior to becoming a Special Agent with HSI, I was employed as a Special Agent with the United States Drug Enforcement Administration ("DEA") for approximately three years. In that capacity, I investigated violations of the Controlled Substances Act, Title 21, U.S.C., §801, et seq., and related offenses. Based on my training and experience, I am familiar with, and have participated in, investigations and search warrants involving narcotics smuggling and trafficking, counterfeit pharmaceuticals smuggling and trafficking, international money laundering, wire fraud, and bank fraud. Furthermore, I am familiar with methods of investigating organizations involved in money laundering and narcotics trafficking, and have become familiar with their methods of operation, including, but not limited to: methods of communication across various digital and telephonic platforms; methods of concealing sources of income; methods of placing, concealing, layering, and integrating laundered currency; methods of manufacturing, importing, cultivating, storing, and selling narcotics; and methods of avoiding detection by law enforcement. In addition, I have received training in the detection and investigation of federal violations at the DEA Academy in Quantico, Virginia.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

PURPOSE OF AFFIDAVIT

3. This affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of digital devices[1] or other electronic storage media[2], described below and in Attachment A, respectively, which is attached hereto and incorporated by reference:

a. A gray OnePlus cellphone, IMEI number 864737041270887, belonging to Colby SMITH, (hereinafter, "**SUBJECT DEVICE 1**"), which is described in Attachment A; and

b. A gray Toshiba Laptop Model S75-A7221, belonging to Colby SMITH, (hereinafter, "**SUBJECT DEVICE 2**"), which is described in attachment A.

4. The **SUBJECT DEVICES** are currently located in the secure evidence vault of the Immigration and Customs Enforcement located in Seattle, WA. Further, the devices have either been shut off or place into "Airplane Mode" to preserve device contents and the state of the device as seized.

5. For the reasons set forth herein, I submit there is probable cause to believe that search of the **SUBJECT DEVICES** will reveal evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, §545 (Smuggling of Goods into the United States), Title 19, United States Code, §1595a(c)(2)(A) (Merchandise Introduced Contrary to Law), Title 18 United States Code §541 (Entry of Goods Falsely Classified), and Title 18 United States Code §542 (Entry of Goods by Means of False Statements) (collectively, the "Subject Offenses").

---

[1] "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

[2] Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

6. The facts set forth in this Affidavit are based on the following: my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of witnesses; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience.

7. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a warrant to search the **SUBJECT DEVICES** for the evidence described in Attachment B, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are relevant to the determination of probable cause to believe that evidence, fruits, and/or instrumentalities of violations of the Subject Offenses will be found in the **SUBJECT DEVICES.**

BACKGROUND ON KAMAGRA SILDENAFIL ORAL JELLY

8. Based upon your affiant's research of the pharmaceutical product Kamagra Sildenafil Oral Jelly, I know the following:

9. Kamagra is the branded name for an erectile dysfunction treatment that contains the ingredient sildenafil. Sildenafil is the same active ingredient contained in the erectile dysfunction treatment Viagra. Kamagra is produced by the company Ajanta Pharma Limited in India and is marketed as a cheap alternative to Viagra. Kamagra is available in the form of tablets, capsules, and flavored jellies.

10. According to the United States Food and Drug Administration ("FDA") [3], a general warning was issued on March 16, 2018, for consumers not to purchase or use drugs advertised as an alternative to Viagra. The FDA indicated that these unapproved drugs which do not meet the stringent standards of the FDA-approved Viagra, contain 100 mg of sildenafil. When improperly taken, the drug can cause adverse reactions. Further,

[3] See the FDA's warning of sildenafil at: https://www.fda.gov/drugs/drug-safety-and-availability/fda-warns-consumers-not-use-unapproved-erectile-dysfunction-products-advertised-radio

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

medications purchased from unapproved and/or unlicensed sources may be dangerous as they can be counterfeit, contaminated, improperly stored and transported, ineffective, and/or unsafe.

11. According to the FDA's list of approved drug products as of March 20, 2020[4], Ajanta Pharma received approval for sildenafil in the form of 25mg, 50mg, and 100mg tablets for the purpose of treating erectile dysfunction. These approvals were received between May 4, 2018 and October 12, 2018. No other forms of sildenafil, such as flavored jellies, were approved by the FDA. Therefore, Kamagra Sildenafil Oral Jelly can only be purchased online from unapproved venders as it is not offered by legitimate pharmacies in the United States.

12. This HSI investigation is conducted in regards to Kamagra Sildenafil Oral Jelly.

//

//

//

[4] See the FDA's list of approved drug products at: https://www.fda.gov/media/136324/download

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

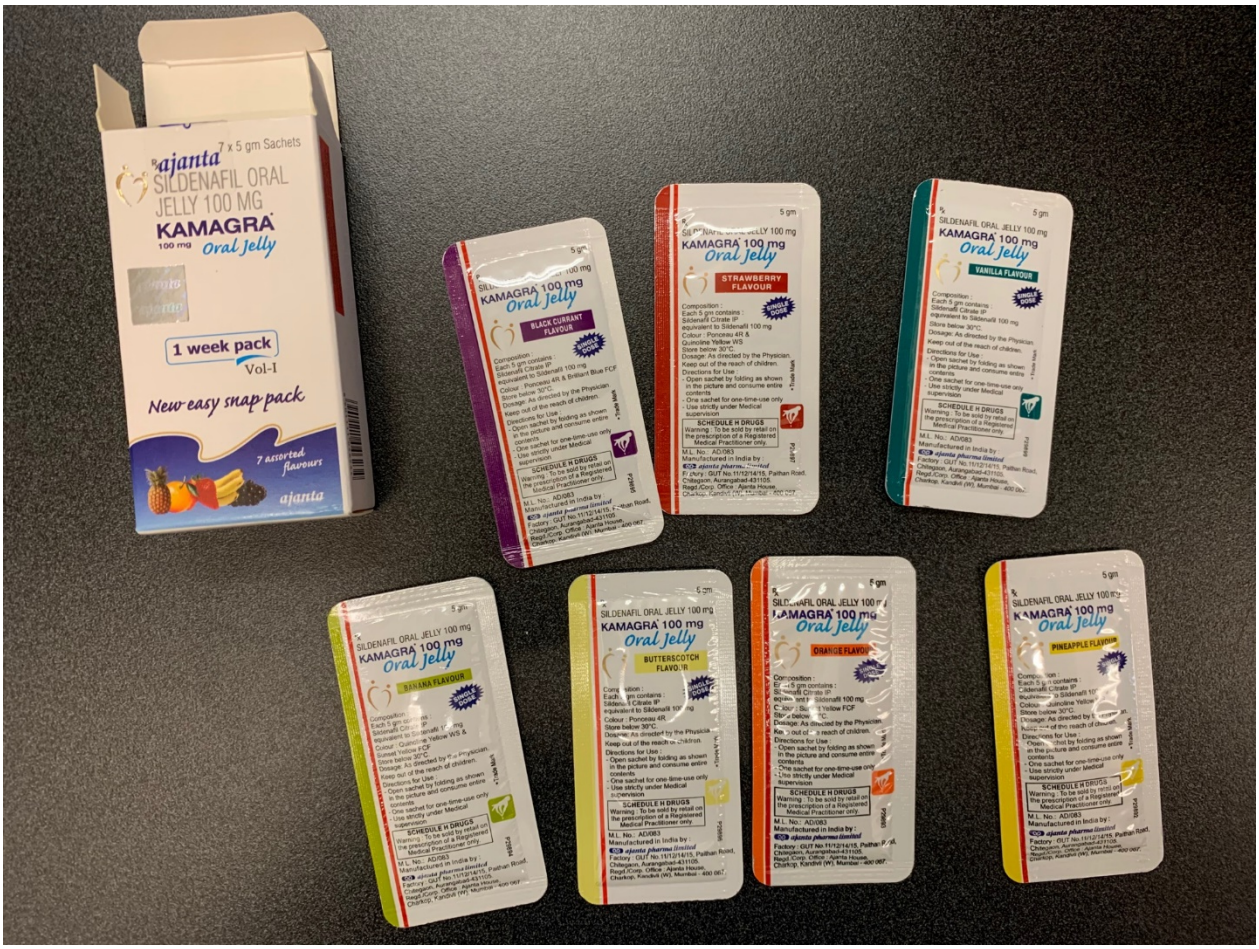

Photo of Kamagra Sildenafil Oral Jelly seized by HSI

STATEMENT OF PROBABLE CAUSE

13. HSI is investigating the suspicious bulk importation of the pharmaceutical product Kamagra Sildenafil Oral Jelly (hereinafter, "SUBJECT NARCOTIC"), which is sourced and imported internationally and mailed to Colby J. SMITH, a Seattle resident who resides at 6020 37th Ave NE, Seattle, WA. As set forth below, the SUBJECT NARCOTIC contains sildenafil which is used to treat male erectile dysfunction by increasing blood flow to the penis. Sildenafil is the same active ingredient found in the United States Food and Drug Administration approved medication Viagra, which requires a medical prescription. Between February 27, 2020 and May 28, 2020, HSI seized four packages containing the SUBJECT NARCOTIC at a gross weight of approximately 13.75 kg. The packages were

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

shipped from Singapore by individuals and/or companies without a clear relation to the pharmaceutical industry, were declared on customs forms as "health supplements" or "supplements," and were indicated to have a declared value well below the sale price of the narcotic. To date, HSI has identified 60 packages between February 5, 2019 and June 15, 2020 addressed to SMITH at his residence which have similar identifiers to previously seized packages.

14. On August 3, 2020, investigators executed a federal search warrant at the residence of SMITH located at 6020 37th Ave NE, Seattle, WA, authorized by United States Magistrate Judge Brian A. Tsuchida on July 31, 2020. At approximately 6:02 a.m., investigators wearing clearly displayed "police" markings executed the aforementioned federal search warrant. Investigators announced their presence and purpose at the residence in a clear and concise manner. At the same time, a Seattle Police Department marked patrol vehicle turned on its lights. Shortly after knocking on the door, a male and female later identified as Colby SMITH (01/XX/1976) and Melissa Ann LEE (09/XX/1975) opened the door. Both individuals were then placed into handcuffs in the front yard of the residence while investigators secured the interior of the residence without incident. Once the residence was secured, investigators labeled each room and took photos of the residence. A thorough and systematic search of the residence was then conducted. While a search of the residence was conducted, your affiant and Postal Inspector (PI) Mitch Vanicek conducted interviews with LEE and SMITH on the back porch.

15. At approximately 6:20 a.m., your affiant and PI Vanicek interviewed LEE. Prior to any questioning, PI Vanicek read LEE her Miranda warnings from a Miranda warning and waiver card. PI Vanicek paused after each warning and asked whether she understood. LEE stated she understood her rights and still wished to speak with investigators. LEE stated in sum to investigators that she was a dentist and owned her own dental practice. LEE stated SMITH is her husband and she was aware SMITH had received several shipments of Kamagra Sildenafil narcotics over the last couple years. LEE stated she did not utilize the narcotics in her practice. LEE stated she saw the parcels containing

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Kamagra in her residence but she did not open them. She stated that she thought SMITH was the one who opened them. When pressed for details regarding the purpose of receiving the Kamagra, use of Kamagra, or whether the Kamagra would be distributed upon receipt, LEE stated she did not know the answers and investigators would have to ask SMITH. LEE stated SMITH worked for MFUSED, a company located in Georgetown Seattle that produced marijuana vape cartridges. After the conversation with investigators, LEE was allowed to leave the residence for the purpose of going to work.

16. At approximately 6:30 a.m., SA Chin and PI Vanicek interviewed SMITH. Prior to any questioning, PI Vanicek read SMITH his Miranda warnings from a Miranda warning and waiver card. PI Vanicek paused after each warning and asked whether he understood. SMITH stated he understood his rights and still wished to speak with investigators. SMITH stated in sum to investigators that he was surfing the internet and found a website which sold Viagra. SMITH e-mailed the website and ordered Viagra. An individual from the website then e-mailed SMITH back and SMITH briefly mentioned he worked in the supply chain industry. The individual from the website then asked SMITH to import Kamagra Sildenafil. The individual from the website stated they represented Ajanta Pharma, which is the same Indian-based company which produced Kamagra. SMITH stated he agreed to receive parcels of Kamagra and reship them to various locations in the United States. SMITH stated he mainly shipped Kamagra to sex shops throughout the country utilizing U.S. Mail. SMITH stated the two people he communicated with from the company were "MIKE" and "YOGI" via WhatsApp on his cellphone, **SUBJET DEVICE 1**. SMITH did not know their last names, but stated that these individuals seemed to know each other and ongoing discussions with SMITH.

17. SMITH stated that he intended to make the import business legitimate and inquired about establishing a Tax ID number. However, "MIKE" and "YOGI" could not provide SMITH a Tax ID number, discouraged him from obtaining a Tax ID number, and asked him not to include his profits from Kamagra sales on his taxes. SMITH then stated that this was a red flag, but he continued to work with them. SMITH stated "MIKE" and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

"YOGI" agreed to pay him $15 for each box he reshipped for them. SMITH would receive the Kamagra shipments, repackage the Kamagra, and then ship the Kamagra using prepaid shipping labels provided by "MIKE" and "YOGI". When asked how SMITH would be paid, SMITH showed investigators **SUBJECT DEVICE 1**'s screen and said he was paid via Venmo by Rengchen CHEN, with the name "Mr. Grey toy" written underneath. SMITH indicated he sent a couple dozen shipments but was ultimately paid less than promised. SMITH then added he was also paid via PayPal and briefly through a Chase Bank account. SMITH provided the telephone numbers for "MIKE" and "YOGI" as 951-878-9484 and 650-751-2497. SMITH stated he only communicated with "MIKE" and "YOGI," and did not communicate with anyone else.

18. SMITH stated he started receiving the Kamagra parcels and reshipping them a couple years ago. SMITH claimed he eventually got to the point where he didn't want to do it anymore and told "MIKE" and "YOGI" he wanted to stop. However, the parcels kept coming to SMITH's residence. SMITH stated he even tried to ignore messages from "MIKE" and "YOGI" but the parcels would still arrive. SMITH claimed that he received the seizure notices from CBP regarding the previously seized Kamagra packages, but the packages still arrived out of his control.

19. When asked if SMITH had ever used Kamagra, SMITH stated that he did a side by side comparison of Kamagra and Viagra. SMITH said "Kamagra beats the shit out of Viagra." Smith added that people shouldn't use it if you didn't need it "or you wouldn't be able to do a raid like this...you will be walking around with wood all day."

20. SMITH asked if we would explain the warrant to him. PI Vanicek stated he could not give SMITH legal advice. Investigators then presented SMITH a copy of the warrant and told him that if he wished legal advice, he should ask a lawyer to review the warrant with him.

21. Investigators then asked SMITH if **SUBJECT DEVICE 2,** found by investigators in a blue backpack in the living room belonged to SMITH. SMITH confirmed it was his laptop which he used for work, and occasionally for personal use as well. When

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

informed that investigators would be seizing **SUBJECT DEVICES 1 and 2** for the purpose of obtaining a warrant to conduct a forensic examination, SMITH pleaded with investigators to not take his devices. SMITH then stated investigators could look through his devices to determine if taking the devices were necessary. SMITH then provided the laptop password as "MZRDIS123" and also provided the phone passcode. However, the devices were ultimately seized. The interview with SMITH was then terminated. It should be noted that within the same blue backpack which belonged to SMITH, investigators observed a CBP seizure notice letter corresponding to a previous Kamagra seizure. Investigators also observed a printer in an upstairs office room which was accessible by SMITH to print prepaid labels as he indicated in the interview.

22. Upon SMITH leaving the residence, SMITH asked PI Todd Salter and PI Justin Lothyan how much money this investigation was costing. PI Salter informed SMITH that he had no idea about any costs involved. SMITH then stated he asked the people to "stop shipping stuff" to him, but they continued to ship it anyways. SMITH asked what he was supposed to do in that circumstance. PI Lothyan then stated he could have shipped the items back or refused to accept the items from the United States Postal Service. SMITH then got into his vehicle and left the residence.

23. At approximately 9:15 a.m., investigators concluded the search of the residence and left a copy of the search warrant, as well as a DHS Form 6051S. DHS Form 6051S listed the item seized from the residence. A complete list of narcotics seized are below:

Item Description	**Quantity of Item Seized**	**Individual Count of Pills**	**Gross Weight of Narcotics**
Ajanta Pharma Kamagra Sildenafil Oral Jelly 100mg (SUBJECT NARCOTIC)	433 Boxes	3,031 Pills	25,400 g
All Day Pharma Stallegra Sildenafil Citrate 100mg Tablets	35 Blister Packs	350 Pills	289 g
Passion Herbal Coffee for Men Single Dose	97 Packs	N/A	2,906 g
Ladygra Sildenafil Citrate 100mg Tablets	140 Blister Packs	560 Pills	646 g
Ajanta Pharma Kamagra Sildenafil Citrate Chewable Tablets	411 Boxes	1,644 Pills	4,290 g

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Ajanta Pharma Super Kamagra (Sildenafil 100mg + Dapoxetine 60mg)	129 Boxes	516 Pills	996 g
Ajanta Pharma Kamagra Gold Sildenafil Citrate Tablets IP	384 Boxes	1,536 Pills	5,088 g

24. A complete list of non-narcotics seized are below:

Item Description	**Quantity of Item Seized**
SUBJECT DEVICE 1	1
SUBJECT DEVICE 2	1
Cell Phone owned by LEE	1
Shipping Labels and Receipts	1 Bundle
Shipping Boxes Addressed to SMITH	1 Bundle
Empty Boxes of Ajanta Pharma Kamagra Gold Sildenafil Citrate Tablets IP	95

25. Based on my training and experience, and interview with SMITH, I have learned that SMITH communicated with individuals he could not fully identify to redistribute bulk Sildenafil narcotics, which were not approved by the FDA or imported contrary to traditional means. SMITH received both the SUBJECT NARCOTIC, as well as variations of Sildenafil narcotics via United States mail, and then shipped the narcotics to sex shops nationwide. SMITH told investigators that **SUBJECT DEVICE 1** was utilized to communicate with individuals who coordinated where narcotics needed to be distributed. Based on my training and experience, criminals are known to conduct their criminal acts utilizing various mobile devices to conceal their communications, sources of narcotics, distribution of narcotics, and flow of illegal proceeds. Therefore, I believe the **SUBJECT DEVICES** contain evidence of SMITH's importation of unlicensed narcotics and distribution of unlicensed narcotics.

TECHNICAL TERMS

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

d. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device

e. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

27. Based on my training, experience and research, I know that the **SUBJECT DEVICES** have capabilities that allow them to serve as a wireless telephone, digital camera, GPS navigation device and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

28. Based on my knowledge, training, and experience, I know that digital devices and electronic storage media can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device used to access the Internet. This information can sometimes be recovered with forensic tools.

29. There is probable cause to believe that things that were once stored on the **SUBJECT DEVICE 2** may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly, apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

30. *Forensic evidence:* As described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **SUBJECT DEVICES** were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **SUBJECT DEVICES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner and/or others with direct physical access to the computer. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.[5] Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's

[5] For example, if the examination of a computer shows that: a) at 11:00am, someone using the computer used an internet browser to log into a bank account in the name of John Doe; b) at 11:02am the internet browser was used to download child pornography; and c) at 11:05 am the internet browser was used to log into a social media account in the name of John Doe, an investigator may reasonably draw an inference that John Doe downloaded child pornography.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

31. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

DIGITAL DEVICES AS INSTRUMENTALITIES OF THE CRIMES

32. Based on my investigation of this case, I know that Colby SMITH has used one or more digital devices in various ways to advance his smuggling of goods into the United States. This has included the use of digital devices to: (1) contact his suppliers via email and cellular phone based applications; (2) receive payment for repackaging and shipping the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

product on internet based applications such as PayPal and Venmo; and (3) use the digital devices to access and/or print out labels to ship the products.

SEARCH TECHNIQUES

33. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit imaging or otherwise copying all data contained on the **SUBJECT DEVICES**, and will specifically authorize a review of the media or information consistent with the warrant.

34. In accordance with the information in this affidavit, law enforcement personnel will execute the search of the **SUBJECT DEVICES** pursuant to this warrant as follows:

a. **Securing the Data**

i. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of the **SUBJECT DEVICES**.[6]

ii. Law enforcement will only create an image of data physically present on or within the **SUBJECT DEVICES**. Creating an image of the **SUBJECT DEVICES** will not result in access to any data physically located elsewhere. However, **SUBJECT DEVICES** that have previously connected to devices at other locations may contain data from those other locations.

//

//

[6] The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. **Searching the Forensic Images**

i. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit.

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CONCLUSION

35. Based on the foregoing, and my training and experience, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, §545 (Smuggling of Goods into the United States), Title 19, United States Code, §1595a(c)(2)(A) (Merchandise Introduced Contrary to Law), Title 18 United States Code §541 (Entry of Goods Falsely Classified), and Title 18 United States Code §542 (Entry of Goods by Means of False Statements), are located in the **SUBJECT DEVICES**, as more fully described in Attachment A to this Affidavit. I therefore request that the court issue a warrant authorizing a search of the **SUBJECT DEVICES** for the items more fully described in Attachment B, respectively, incorporated herein by reference, and the seizure of any such items found therein.

ERIC CHIN
Special Agent
Homeland Security Investigations

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit by telephone on this 19th day of August, 2020.

HON. Mary Alice Theiler
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Devices To Be Searched

a. A gray OnePlus cellphone, IMEI number 864737041270887, belonging to Colby SMITH, ("**SUBJECT DEVICE 1**"), and

b. A gray Toshiba Laptop Model S75-A7221, belonging to Colby SMITH, ("**SUBJECT DEVICE 2**").

The **SUBJET DEVICES** are currently located in the secure evidence vault of Immigration and Customs Enforcement located in Seattle, WA. Further, the devices have either been shut off or placed into "Airplane Mode" to preserve device contents and the state of the device as seized.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

List of Items to be Searched for and Seized in the SUBJET DEVICES

The following items, which constitute fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, §545 (Smuggling of Goods into the United States), Title 19, United States Code, §1595a(c)(2)(A) (Merchandise Introduced Contrary to Law), Title 18 United States Code §541 (Entry of Goods Falsely Classified), and Title 18 United States Code §542 (Entry of Goods by Means of False Statements), including:

1. All records on the **SUBJECT DEVICES** described in Attachment A that relate to violations of Title 18, United States Code, §545 (Smuggling of Goods into the United States), Title 19, United States Code, §1595a(c)(2)(A) (Merchandise Introduced Contrary to Law), Title 18 United States Code §541 (Entry of Goods Falsely Classified), and Title 18 United States Code §542 (Entry of Goods by Means of False Statements) and involve Colby SMITH, including:

   a. Lists of customers and related identifying information;

   b. Any and all financial accounting records to include check registers, general journals, and supporting journals, logs, spreadsheets, general ledgers, schedules, checks, remittance advices, receipts, invoices mailings, envelopes, tax returns, financial statements and other related documentation involving the buying and selling of Kamagra Sildenafil Oral Jelly, or pharmaceuticals and supplements suspected to contain sildenafil from February 5, 2019 to present;

   c. Any and all bank account records and other information showing the receipt and disbursement of funds to include cancelled checks, deposit and withdrawal slips, cashier's checks, advice of debit/credit, and orders for telegraphic or electronic payment or transfer; safe deposit box numbers and entry records; certificates of deposit, bonds, notes and/or acceptances; wire transfers, bank statements, account applications and all other bank documents including

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

correspondence, notes, and memoranda, related to transactions, persons or business entities, or accounts from February 2019 to present;

d. Evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

e. Evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

f. Evidence of the lack of such malicious software;

g. Evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

h. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

i. Evidence of the times the digital device or other electronic storage media was used;

j. Passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

k. Documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

l. **SUBJECT DEVICE 1** may be searched only for the following items:

   i. Assigned number and identifying telephone serial number (ESN, MIN, IMSI, or IMEI);

   ii. Stored list of recent received, sent or missed calls

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

iii. Stored contact information;

iv. Stored files (including photographs and videos) displaying or accounting for currency, banking transactions, financial records, shipping information, mail, evidence of the aforementioned offense, and/or that may show the user of **SUBJECT DEVICE 1** and/or coconspirators, including any embedded GPS data associated therewith;

v. Stored text message and stored emails that are evidence of the aforementioned crimes, including similar messaging services saved by third party applications stored on the telephone (such as WhatsApp, Signal, Wickr, and Telegram);

vi. Evidence of user attribution showing who used or owned **SUBJECT DEVICE 1** at the time the items described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, and documents;

vii. Records and information evidencing bank transactions;

viii. Records of Internet Protocol (IP) addresses used;

ix. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user typed web addresses

m. Any mail, packaging, shipping or receiving documents, records, documents or communication, in whatever form, that refer to shipments by Colby SMITH that are part of the smuggling scheme relating to the above crimes;

When executing the warrant, the United States may use the passwords provided by the user of the **SUBJECT DEVICES** at the time it was seized by law enforcement agents.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970